Claims

1. A method for providing a secure computing environment, comprising:

providing an encryption control device, the encryption control device being in communication with a computer and a smart card;

authenticating a user as a valid owner of the smart card;

initializing the encryption control device through a challenge/response protocol with the smart card if the valid owner is authenticated; and

activating an encryption/decryption engine of the encryption control device to enable access to data in a secure computing environment if the challenge response protocol is executed successfully.

2. The method as recited in claim 1, wherein the authenticating a user as a valid owner of the smart card includes providing a personal identification number.

3. The method as recited in claim 1, wherein the authenticating a user as a valid owner of the smart card includes providing a biometric identifier.

4. The method as recited in claim 1, wherein the challenge/response protocol includes an exchange of private and public keys between the encryption control device and a smart card.

5. The method as recited in claim 1, wherein a biometric scanner is employed for authenticating a user.

6. The method as recited in claim 1, further including,

monitoring for continued presence of the valid owner; and

locking the encryption control device if the valid owner is not detected.

7. The method as recited in claim 1, wherein the smart card stores the user's personal data.

8. The method as recited in claim 1, wherein a personal identification number is used to authenticate a user.

9. The method as recited in claim 1, further including,

providing control switches for bypassing the encryption control device.

10. A method for activating an encryption control device that is in communication with a computer for providing a secure computing environment for a user, comprising:

providing a card for insertion into a card reader of the encryption control device, the card being configured to receive and pass data;

receiving a biometric identifier from the user, the biometric identifier enabling validation of the user as the authorized owner of the card;

running a challenge/response protocol between the encryption control device and the inserted card, the challenge response protocol establishing that the inserted card and the encryption control device are compatible; and

activating an encryption engine of the encryption control device to create a secure computing environment if the user is validated as the authorized owner of the card and challenge response protocol is successfully executed.

11. The method as recited in claim 10, wherein the encryption control device is portable.

12. The method as recited in claim 10, wherein the encryption engine executes RSA public-key cryptosystem.

13. The method as recited in claim 10, wherein the encryption control device is hot plugable.

14. The method as recited in claim 10, wherein the data are public and private keys.

15. The method as recited in claim 10, further including;

providing a system tray utility program for allowing the user to control and customize encryption control device security features.

16. The method as recited in claim 10, wherein execution of the challenge/response protocol establishes a secure path between the encryption control device and the inserted card, the secure path allowing for configuration and biometric data from the encryption control device to be transferred to the inserted card and allowing data from the inserted card to downloaded to the encryption control device.

17. A method for operating a computer in a secure mode, comprising:

providing an encryption control device, the encryption control device (ECD) being in communication with the computer and a smart card, the encryption control device storing a biometric identifier of a user;

authenticating the user as a valid owner of the smart card, the authenticating further including,

receiving a biometric identifier from the user, and

comparing the received biometric indicator with the stored biometric indicator for a match; and

activating an encryption engine of the encryption control device to create a secure operating mode if the user is authenticated.

18. The method as recited in claim 16, wherein the ECD includes a storage medium for storing encrypted data.

19. The method as recited in claim 16, wherein encrypted data is stored on a virtual drive of the computer.

20. The method as recited in claim 16, further including;

allowing the user to transfer unencrypted data from a non-secure storage drive to a secure storage drive, the secure storage drive storing data in an encrypted format.